

[First Hit](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L7: Entry 2 of 8

File: PGPB

Feb 24, 2005

DOCUMENT-IDENTIFIER: US 20050044199 A1

TITLE: Storage network management system and method

Abstract Paragraph:

In a computer system having a storage device, switches and hosts respectively connected by a network, in accordance with an ID of a logical volume of the storage device and an IP address of a host, access control configuration of the logical volume is performed relative to the storage device, the IP address of the host is converted into a MAC address, the MAC address of the host is converted into a port ID of the switch connected to the host, and addition of the port to virtual local area network (VLAN) is performed for the switch. Logical unit number (LUN) masking and VLAN configuration essential for security countermeasure of IP-SAN (Internet protocol-storage area network) can be managed collectively by a system administrator so that the running cost of IP-SAN can be lowered.

Summary of Invention Paragraph:

[0004] Attention has been paid recently to network storage technology, IP-SAN (Internet Protocol-Storage Area Network), which uses an IP network whose initial cost is cheaper than that a network using Fibre Channel (hereinafter abbreviated to "FC"). The IP network requires, however, an additional cost for maintaining security because many security threatening crack tools are circulated.

Summary of Invention Paragraph:

[0005] As the security countermeasure for a conventional FC-SAN, LUN (Logical Unit Number) masking has been used. The LUN masking is the technique according to which access from a computer to a logical unit (Logical Unit, hereinafter abbreviated to LU) of a storage device is restricted by the storage device to prevent illegal data reference, alteration and erase.

Summary of Invention Paragraph:

[0006] If the LUN masking technique of FC-SAN is to be realized in IP-SAN, a computer accessible to each LUN of a storage device is designated by an IP address assigned to the computer. It is, however, easy to tap a packet sent/received to/from another computer connected to the same subnet in the IP network. Therefore, if the same network is shared by two or more departments or businesses, data security is impossible to be ensured, and the configuration of only the LUN masking is insufficient for the security countermeasure. It is therefore necessary to use other security techniques together with the LUN masking.

Summary of Invention Paragraph:

[0007] A candidate for the security technique to be used with the LUN masking may be data cryptograph utilizing IPSec techniques or the like. However, a cryptography process has a large load on a CPU. If this process is applied to IP-SAN, the I/O performance of a storage device is degraded. In order to suppress such performance degradation, although the cryptography process may be executed by using dedicated hardware, this approach is unsatisfactory for the security technique to be used together with the LUN masking because it requires a high initial cost.

Summary of Invention Paragraph:

[0008] Another candidate for the security technique may be VLAN (Virtual Local Area

Network) techniques according to which one physical network is divided into a plurality of logical networks. With the VLAN techniques, one or more computers such as those used by the same department posing no problem of data tapping are classified into one group. Each group is assigned a logical network to prevent data tapping by other groups. VLAN has been adopted by most of LAN switches so that there is no additional initial cost. It can therefore be expected that a combination of LUN masking and VLAN technologies will be used as the security countermeasure of IP-SAN.

Summary of Invention Paragraph:

[0010] The configuration work of LUN masking and VLAN is required to be performed not only on the side of a storage device but also on the side of switches in IP-SAN. Since the configuration work is required on the sides of different devices, a system user or administrator has a large work load.

Summary of Invention Paragraph:

[0014] According to one embodiment of the invention, a management method for a storage system having a storage device, a switch and a computer respectively connected by a network, comprises a step of, in accordance with an identifier of a storage area of the storage device and a first address of the computer, performing a configuration of an access control to the storage area of the storage device, converting the first address of the computer into a second address, converting the second address of the computer into an identifier of a port of the switch connected to the computer, and adding the identifier of the port to a virtual LAN for the switch.

Detail Description Paragraph:

[0029] First, description will be made on a computer system according to a first embodiment of the invention. In the first embodiment, IP-SAN security is managed by a storage management device which manages the configuration of a storage device and monitors the storage device.

Detail Description Paragraph:

[0036] The switch 3 has a controller which receives configuration information of VLAN from an external to perform the configuration of VLAN. The controller of the switch 3 sends a forwarding database in response to a request from an external and notifies link-down to an external.

Detail Description Paragraph:

[0038] The main memory 21 stores various programs to be executed by CPU 24. More specifically, the programs include: a GUI control program 10 to be executed by CPU 24 when a graphical user interface is supplied to a system administrator; a discovery_request receiving program 11 to be executed when registration is received from an iSCSI target and when a discovery_request of an iSCSI target from an iSCSI initiator (host) is received and responded; an ARP transmitting program 12 to be executed when the storage management device 1 performs translation between an IP address and a MAC address by using ARP (Address Resolution Protocol, RFC826); a port ID retrieving program 13 to be executed when a forwarding database is retrieved from the switch 3 and the MAC address is converted into a port ID which is an ID of a physical port; a LUN masking configuring program 14 to be executed when the LUN masking is configured for the storage device 2; and a VLAN configuring program 15 to be executed when the VLAN configuration is performed for the switch 3.

Detail Description Paragraph:

[0076] The details of the address table updating process will be given. First, the storage management device 1 broadcasts an ARP request via the communication lines 20a. At this time, since the communication line 20a interconnecting the storage management device 1 and switch 3a and the communication line 20a interconnecting the physical ports 41 and 42 belong to the same VLAN, the broadcast packet reaches

the physical port 41 (S602).

Detail Description Paragraph:

[0082] In this communication sequence, first the host 4a sends a service request to the storage management device 1 to acquire a usable iSCSI target (S611) and lastly the storage management device 1 sends the usable iSCSI target to the host 4a via the communication line 20a (S618). The other communication sequence is similar to that shown in FIG. 6A. In the communication sequence to be performed when the host 4c or 4d is connected to the switch 3b, the switch 3b is inserted between the host 4 and switch 3a, and the other communication sequence is similar to that shown in FIG. 6A.

Detail Description Paragraph:

[0086] Lastly, the storage management device 1 performs the VLAN deleting process. In the VLAN deleting process, the storage management device 1 sends a VLAN configuration request to the switch 3a via the communication line 20b in order to delete the physical port of the host 4 or storage device 2 whose link was disconnected (S623, S624).

Detail Description Paragraph:

[0089] Upon reception of the service advertisement packet or service request packet, the storage management device 1 executes the service request reception program 11 to acquire an IP address of a packet sender from the received service advertisement packet or service request packet (S701).

Detail Description Paragraph:

[0090] Next, the storage management device 1 executes the ARP sending program 12 to assemble an ARP request of inquiring the MAC address of the IP address obtained at S701 and to broadcast it via the communication lines 20a (S702). Upon reception of the ARP response to the ARP request issued at S702, the storage management device 1 executes the ARP sending program 12 to derive the MAC address from the ARP response (S703).

Detail Description Paragraph:

[0091] Next, the storage management device 1 executes the port ID acquiring program 13 to fetch the first record of the switch table 35 (S704) and to send an acquisition request of the forwarding database to the management IP address of the record via the communication line 20b. For example, the acquisition request of the forwarding database can be realized by acquiring an ipNetToMediaTable of MIB-2 (Management Information Base-2, RFC1213) by using Get of SNMP (Simple Network Management Protocol) (S705).

Detail Description Paragraph:

[0095] First, the storage management device 1 executes the VLAN configuring program 15 to derive the iSCSI name of the iSCSI target or the IP address of the iSCSI initiator from the service advertisement packet or the service request packet respectively received at S701 shown in FIG. 7 (S801).

Detail Description Paragraph:

[0097] Next, the storage management device 1 searches again the group membership table 32 by using the group ID acquired at S802 as a search key (S803). If this search result indicates that the iSCSI target or the iSCSI initiator used as a key for searching the group ID is the first iSCSI node of the group, i.e., if the search at S803 indicates that the values of the connection flags in the entries 323 of all records are "0" (S804), the storage management device 1 sends a VLAN configuring request of creating a VLAN having the group ID acquired at S802 as its VLAN ID, to the switch via the communication line 20b (S805).

Detail Description Paragraph:

[0098] After the step at S805 or if the value in the entry 323 of any record is "1"

at S804, the storage management device 1 sends a VLAN adding request of adding the port ID acquired at S707 shown in FIG. 7 to the created (or already existing) VLAN via the communication line 20b. The destination of this VLAN configuring request or VLAN adding request is the management IP address 351 of the record acquired at S704 or S710 shown in FIG. 7 (S806).

Detail Description Paragraph:

[0103] If the search at S903 or S904 does not find a record (S905), the storage management device 1 terminates the process. If a record is found at S905, the storage management device 1 derives the group ID from the found record. The storage management device 1 sends a VLAN releasing request to the switch via the communication line 20b, the VLAN releasing request deleting the port ID contained in the link-down notice at S621 shown in FIG. 6C from the VLAN having the derived group ID as its VLAN ID (S906).

Detail Description Paragraph:

[0105] Next, the storage management device 1 searches again the group membership table 32 by using the group ID acquired at the preceding step as a search key (S908). If this search result indicates that the iSCSI target or iSCSI initiator is the last iSCSI node of the group, i.e., if the search at S908 indicates that the values of the connection flags in the entries 323 of all records are "0" (S909), the storage management device 1 sends a VLAN deleting request of deleting VLAN corresponding to the group ID, to the switch via the communication line 20b (S910).

Detail Description Paragraph:

[0106] Thereafter, if necessary, the storage management device 1 may send a packet for storing or validating the switch configuration to the switch 3. The destination of the VLAN releasing request at S906 or the VLAN deleting request at S910 is the management IP address 351 in the switch table 35 acquired at S622 of FIG. 6C.

Detail Description Paragraph:

[0107] According to the first embodiment described above, a system administrator configures LUN masking and enters a subnet address of VLAN to which the host 4 and storage device 2 constituting a group belong. With only these works by the system administrator, the storage management device 1 automatically instructs a switch to create VLAN when the host 4 or storage device 2 is connected to the network. The work load for security countermeasure of IP-SAN by the system administrator can therefore be reduced considerably.

Detail Description Paragraph:

[0108] Next, a second embodiment will be described. Only different points from the first embodiment will be described. In the second embodiment, the above-described IP-SAN security management is performed by a switch 3.

Detail Description Paragraph:

[0109] FIG. 10 is a diagram showing the configuration of a computer system having a storage device 2, switches 3a and 3b and hosts 4a, 4b, 4c and 4d, respectively connected by communication lines 20a. The storage device 2, switches 3a and 3b are also interconnected by communication lines 20b. In the following, it is assumed that the switch 3a performs the IP-SAN security management.

Detail Description Paragraph:

[0110] The switch 3a has: data send/receive elements 50 for receiving data from a network and sending data to the network or a data switching element 51 which is a bus or crossbar switch for sending/receiving data to and from the two data send/receive elements data 50; a forwarding database storage 52; a data switching controller 53 for controlling a data transmission destination of the data send/receive element in accordance with the contents of the forwarding database storage 52; a GUI controller 10, a discovery request receiver 11, an ARP sender 12,

a port ID retriever 13, a LUN masking configuration element 14; a VLAN configuration element 15 and a main memory 21.

Detail Description Paragraph:

[0115] After the host 4a is connected to the switch 3a, the host 4a first sends a service request to the switch 3a (S1101). Upon reception of the service request, the switch 3a sends an ARP request to the host 4a by using the ARP sender 12 to acquire the MAC address of the host 4a (S1102, S1103).

Detail Description Paragraph:

[0117] The VLAN configuration element 15 searches the group key table 31 by using as a key the IP address of the sender of the service request and acquires the group ID 310 of the searched record. The VLAN configuration element 15 requests the data switching element 53 to configure VLAN and add the port ID acquired at S1104 to VLAN having the group ID as its VLAN ID. Thereafter, the data switching element 53 notifies the contents of the received VLAN configuration contents to the data send/receive element 50 so that the data send/receive element 50 can configure VLAN (S1105). Lastly, the discovery request receiver 11 of the switch 3a returns a service response to the host 4a (S1106).

Detail Description Paragraph:

[0119] Next, a third embodiment will be described. In this embodiment, the above-described IP-SAN security management is performed by the storage device 2. In this embodiment, the storage device 2 has the main memory 21 and magnetic disk 23. The main memory 21 stores the GUI controlling program 10, discovery request receiving program 11, ARP sending program 12, port ID retrieving program 13, LUN masking configuring program 14 and VLAN configuring program 15. The magnetic disk 23 stores the address table 30, group table 31, group membership table 32, LUN masking table 33, iSCSI name table 34 and switch table 35. The operation sequence of this embodiment is similar to that of the first embodiment, excepting that the storage management device 1 is replaced with the storage device 2.

Detail Description Paragraph:

[0120] According to the present invention, LUN masking and VLAN configuration of IP-SAN can be controlled collectively so that a load of configuration works by a system administrator can be reduced and a miss occurrence rate can be lowered. The running cost of IP-SAN can therefore be lowered.

CLAIMS:

1. A management apparatus for managing a storage network having a computer, a storage device and a switch, comprising: a controller, an interface connected to said switch and an input interface to be used by an administrator, wherein when said computer or said storage device is connected to said switch: based on information of first and second identifiers of said computer or said storage device acquired via said interface from said computer or said storage device connected to said switch, information of a correspondence relation acquired from said switch via said interface between said second identifier of said computer or said storage device connected to said switch, and a third identifier for identifying an interface of said switch connected to said computer or said storage device, and information regarding said first identifier for identifying said computer or said storage device constituting a predetermined group entered by said administrator via said input interface, said third identifier of said switch belonging to said predetermined group is specified; and in response to inputting of information of a storage area of said storage device and information regarding said first identifier of said computer which can use said storage area, from said input interface, the input information is sent to said storage device to instruct security configuration, information of said third identifier of said switch corresponding to said first identifier and information of said predetermined group to which said third identifier belongs is derived, and the derived information is sent to said

switch to instruct configuration of a virtual LAN corresponding to said predetermined group.

9. A switch connectable to a computer and a storage device, comprising: a controller, an interface connected to said storage device or said computer and an input interface to be used by an administrator, wherein when said computer or said storage device is connected to said interface: in accordance with information of first and second identifiers of said computer or said storage device acquired via said interface from said computer or said storage device connected, information of a correspondence relation possessed by said switch between said second identifier of said computer or said storage device connected to said switch, and a third identifier for identifying an interface of said switch connected to said computer or said storage device, and information regarding said first identifier for identifying said computer or said storage device constituting a predetermined group entered by said administrator via said input interface, said controller identifies said third identifier corresponding to said computer or said storage device belonging to said predetermined group; and in response to inputting of information of a storage area of said storage device and information regarding said first identifier of said computer which can use said storage area, from said input interface, input information is sent to said storage device to instruct security configuration, information of said third identifier corresponding to said first identifier and information of said predetermined group to which said third identifier belongs is derived, a virtual LAN corresponding to said predetermined group is configured.

10. A storage device connectable to a switch connected to a computer, comprising: a controller, an interface connected to said switch, an input interface to be used by an administrator and a storage area, wherein when said computer is connected to said switch: based on information of first and second identifiers of said computer acquired via said interface from said computer connected, information of a correspondence relation acquired from said switch via said interface between said second identifier of said computer connected to said switch and a third identifier for identifying said interface of said switch connected to said computer, and information regarding said first identifier for identifying said computer constituting a predetermined group entered by said administrator via said input interface, said third identifier corresponding to said computer belonging to said predetermined group is identified; and in response to inputting of information of said storage area and information regarding said first identifier of said computer which can use said storage area, from said input interface, security configuration is performed, information of said third identifier corresponding to said first identifier and information of said predetermined group to which said third identifier belongs is derived, and said switch is instructed to configure a virtual LAN corresponding to said predetermined group.

11. A management method for managing a storage network having a computer, a storage device and a switch, comprising the steps of: when said computer or said storage device is connected to said switch: based on information of first and second identifiers of said computer or said storage device acquired from said computer or said storage device connected to said switch, information of a correspondence relation acquired from said switch between said second identifier of said computer or said storage device connected to said switch, and a third identifier for identifying an interface of said switch connected to said computer or said storage device, and information regarding said first identifier for identifying said computer and said storage device constituting a predetermined group, specifying said third identifier corresponding to said computer or said storage device belonging to said predetermined group; and based on information of a storage area of said storage device and information regarding said first identifier of said computer which can use said storage area, performing security configuration by said storage device, extracting information of said third identifier corresponding to said first identifier and information of said predetermined group to which said

third identifier belongs, and creating through said switch a virtual LAN corresponding to said predetermined group.

12. A management method for a storage system having a storage device, a switch and a computer respectively connected by a network, comprising the steps of: based on an identifier of a storage area of said storage device and a first address of said computer, performing access control configuration relative to the identifier of said storage area for said storage device; and converting the first address of said computer into a second address, converting the second address of said computer into an identifier of a port of said switch connected to said computer, and adding the identifier of said port to a virtual LAN for said switch.

13. A management method for a storage system having a storage device, a switch and a computer respectively connected by a network, comprising the steps of: based on an identifier of a storage area of said storage device and a first address of said computer, performing access control configuration for said computer relative to said storage area by said storage device; and converting the first address of said computer into a second address, converting the second address of said computer into an identifier of a port of said switch connected to said computer, and adding the identifier of said port to a virtual LAN for said switch.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L7: Entry 3 of 8

File: PGPB

Jul 8, 2004

DOCUMENT-IDENTIFIER: US 20040133634 A1

TITLE: Switching system

Abstract Paragraph:

A digital network comprises a plurality of data storage elements (104), at least one client (102) and a switch element (106) operable to receive access requests from the client (102) and provide access to data on the storage elements (104) in response to access requests.

Summary of Invention Paragraph:

[0008] Conventional systems, however, do not enable seamless connection and interoperability among disparate storage platforms and protocols. Storage Area Networks (SANs) typically use a completely different set of technology based on Fibre Channel (FC) to build and manage storage networks. This has led to a "re-inventing of the wheel" in many cases. Users are often require to deal with multiple suppliers of routers, switches, host bus adapters and other components, some of which are not well-adapted to communicate with one another. Vendors and standards bodies continue to determine the protocols to be used to interface devices in SANs and NAS configurations; and SAN devices do not integrate well with existing IP-based management systems.

Summary of Invention Paragraph:

[0009] Still further, the storage devices (Disks, RAID Arrays, and the like), which are Fibre Channel attached to the SAN devices, typically do not support IP (and the SAN devices have limited IP support) and the storage devices cannot be discovered/managed by IP-based management systems. There are essentially two sets of management products--one for the IP devices and one for the storage devices.

Summary of Invention Paragraph:

[0010] Accordingly, it is desirable to enable servers, storage and network-attached storage (NAS) devices, IP and Fibre Channel switches on storage-area networks (SAN), WANs or LANs to interoperate to provide improved storage data transmission across enterprise networks.

Summary of Invention Paragraph:

[0018] The invention addresses the noted problems typical of prior art systems, and in one aspect, provides a switch system having a first configurable set of processor elements to process storage resource connection requests, a second configurable set of processor elements capable of communications with the first configurable set of processor elements to receive, from the first configurable set of processor elements, storage connection requests representative of client requests, and to route the requests to at least one of the storage elements, and a configurable switching fabric interconnected between the first and second sets of processor elements, for receiving at least a first storage connection request from one of the first set of processor elements, determining an appropriate one of the second set of processors for processing the storage connection request, automatically configuring the storage connection request in accordance with a protocol utilized by the selected one of the second set of processors, and forwarding the storage connection request to the selected one of the second set of processors for routing to at least one of the storage elements.

Summary of Invention Paragraph:

[0025] The invention, in another aspect, also enables automatic discovery of SCSI devices over an IP network, and mapping of SNMP requests to SCSI.

Brief Description of Drawings Paragraph:

[0051] FIG. 24 depicts load balancing NFS client requests between NFS servers.

Detail Description Paragraph:

[0081] The client abstraction layer isolates, secures, and protects internal resources; enforces external group isolation and user authentication; provides firewall access security; supports redundant network access with fault failover, and integrates IP routing and multiport LAN switching. In addition, it presents external clients with a "virtual service" abstraction of internal services, so that there is no need to reconfigure clients when services are changed. Further, it provides internal services a consistent network interface, wherein service configuration is independent of network connectivity, and there is no impact from VLAN topology, multihoming or peering.

Detail Description Paragraph:

[0082] FIG. 5 provides detail of the client abstraction layer. As shown therein, it can include TCP acceleration function 502 (which, among other activities, offloads processing reliable data streams); load balancing function 504 (which distributes requests among equivalent resources); content-aware switching 506 (which directs requests to an appropriate resource based on the contents of the requests/packets); virtualization function 508 (which provides isolation and increased security); 802.1 switching and IP routing function 510 (which supports link/path redundancy), and physical I/F support functions 512 (which can support 10/100Base-T, Gigabit Ethernet, Fibre Channel and the like).

Detail Description Paragraph:

[0108] Network Processor Config Service (NPCS)--used to receive and process configuration requests.

Detail Description Paragraph:

[0109] Action Manager--used to send and receive requests to execute remote functionality such as rebooting, clearing stats and re-syncing with a file system.

Detail Description Paragraph:

[0119] Management software is a collection of components responsible for configuration, reporting (status, statistics, etc), notification (events) and billing data (accounting information). The management software may also include components that implement services needed by the other modules in the system.

Detail Description Paragraph:

[0131] These components are responsible for communicating with the other cards in the system to get/set data. For example the CSM sends configuration data to a card/processor when a UI initiates a change and receives statistics from a card/processor when a UI requests some data.

Detail Description Paragraph:

[0156] In order to accomplish this IP addresses be assigned to the storage devices (either manually or automatically) and the MIC will have to be sent all IP Mgmt (exact list TBD) packets destined for one of the storage IP addresses. The MIC will then mediate by converting the IP packet (request) to a similar FC/SCSI request and sending it to the device.

Detail Description Paragraph:

[0157] For example an IP Ping would become a SCSI Inquiry while a SNMP get of sysDescription would also be a SCSI Inquiry with some of the returned data (from